Be Aware Be Safe

Nova UA Federal Credit Union is committed to cyber security to help keep you safe online.

Knowledge is the best defense, so check out our cyber security tips.

Online Safety Tips:

*** Watch Out for Fraudulent E-mails**

The emails and text you receive may look official, but they could be fake. Never click on a link or respond to an email or text with personal information — credit card numbers, Social Security numbers, or other banking details; instead contact the company directly or visit online by typing the company's web address into your Internet browser.

*** Choose Passwords Carefully**

Create passwords that are easy to remember, but difficult for others to guess, and change them often. The best passwords are a minimum of eight characters, contain a mix of letters, numbers, spaces and symbols, and use words that are not common. Never use the same password for banking as you do for other sites, such as social media or email.

*** Be Careful What You Share Online**

Personal information shared on social networking sites like Facebook, Twitter, Instagram and LinkedIn can be used by criminals to commit fraud. Never post key information such as where you bank, how you invest your money, physical addresses, emails, cell phone numbers, account numbers or passwords.

*** Guard Your Mobile Device**

Your cell phone contains valuable personal information. Secure it with a password and be sure to wipe it clean before trading it in for a new model. Be careful of scanning QR codes, as they may direct you to a fraudulent site. You can add your mobile phone to the **“Do Not Call”** list at www.donotcall.gov.

*** Avoid Banking from Public Wi-Fi Hotspots**

The Wi-Fi available at many public locations may not be secure. Be cautious about the sites you visit and the information you release.

*** Keep Security Software up to Date**

PCs, laptops, smartphones, tablets and other web-enabled devices need the most current protection from viruses, malware and other online threats. Maintaining the latest security software, web browser and operating system are your best defense.

Extra Security Tips

Social Media

Never use the same password for banking as you do for social media or email. Be careful what you share online. Information shared on social networking sites can be used by criminals to commit fraud or other crimes. Never post information about where and how you bank or when you are away on vacation.

How to know if you are being Phished or Pharmed

Both attacks are attempts to get your usernames and passwords, but they are not the same.

How to Spot a Phish

- Getting asked for personal information via email
- Receiving an email that offers something too good to be true
- Do you see misspelled words or words in ALL CAPS?
- It just does not look like normal company correspondence
- Does the email contain an attachment? Beware of all attachments

How Pharming Works

In a pharming scam, traffic intended for one website is redirected to a fraudulent online address. You can unknowingly become part of a pharming fraud in one of two ways:

- You can be “pharmed” by visiting unfamiliar websites where hackers alter the host files on your computer while you’re visiting.
- You can also be pharmed if a server connected to your computer is compromised and allows your personal online account information to be hacked.

Find out more about how you can protect yourself from identify theft, scams and other type of financial fraud by visiting the government web sites listed below:

https://www.consumer.ftc.gov/features/feature-0038-onguardonline

https://www.dhs.gov/stopthinkconnect-toolkit

https://www.ic3.gov/default.aspx

https://www.us-cert.gov/ncas/tips